UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/609,011 | 06/30/2003 | Jari Karjala | 004770.00133 | 8337 |

22907 7590 02/20/2008
BANNER & WITCOFF, LTD.
1100 13th STREET, N.W.
SUITE 1200
WASHINGTON, DC 20005-4051

| EXAMINER | |
|---|---|
| NGUYEN, MINH DIEU T | |
| **ART UNIT** | **PAPER NUMBER** |
| 2137 | |
| **MAIL DATE** | **DELIVERY MODE** |
| 02/20/2008 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

mn

| | | | |
|---|---|---|---|
| **Office Action Summary** | **Application No.**<br>10/609,011 | **Applicant(s)**<br>KARJALA ET AL. | |
| | **Examiner**<br>MINH DIEU NGUYEN | **Art Unit**<br>2137 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on 24 August 2007.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-3,5,8,10-27,29,32,34-47 and 49-52* is/are pending in the application.

4a) Of the above claim(s) *4,6,7,9,28,30,31,33 and 48* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,5,8,10-27,29,32,34-47 and 49-52* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *4/27 and 11/27/07*.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

## DETAILED ACTION

### *Response to Amendment*

1. This office action is in response to the communication dated 8/24/07 with the amendments to claims 1-3, 5, 8, 10-27, 29, 32, 34-47, the cancellation of claims 4, 6-7, 9, 28, 30-31, 33 and 48 and the addition of claims 49-52.

2. Claims 1-3, 5, 8, 10-27, 29, 32, 34-47 and 49-52 are pending.

### *Information Disclosure Statement*

3. The information disclosure statement filed 4/27/07 and 11/27/07 have been placed in the application file and the information referred to therein has been considered as to the merits.

### *Claim Objections*

4. The objections of claims 1-3, 5, 9, 14, 20, 24-27, 29, 33, 38, 40 and 44 have been withdrawn based on the filed amendments.

### *Claim Rejections - 35 USC § 112*

5. The rejections of claims 1-47 under 35 U.S.C. 112, second paragraph, have been withdrawn based on the filed amendments.

### *Response to Arguments*

6. Applicant's arguments have been considered but are moot in view of the new ground(s) of rejection.

### *Claim Rejections - 35 USC § 103*

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1, 3, 8, 10, 25, 27, 32 and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Corrigan et al. (6,640,097) in view of Tuomenoksa et al. (7,028,333).

a) As to claim 1, Corrigan discloses a method comprising:

(a) initiating a connection via a publicly accessible network from a wireless device, wherein the wireless device includes an unprovisioned virtual private network (VPN) program and an unprovisioned automatic content updating (ACU) program, and the ACU program is configured, upon provisioning, to communicate with one or more remotely-located devices on behalf of at least one additional program that is distinct from the ACU and VPN programs (i.e. a mobile user initiates a connection for service request (Corrigan: Fig. 3); the service request can be service and subscriber provisioning and VPN services (Corrigan: col. 4, lines 31, 44), where provisioning functions includes subscriber self-provisioning, customer care provisioning, device provisioning, service provisioning and subscriber authentication (Corrigan: col. 4, line 47 to col. 5, line 40). It anticipates that the mobile device contains unprovisioned VPN and ACU program before requesting the provisioning services. Upon provisioning, the mobile user can communicate with other program for services (Corrigan: col. 7, lines 33-43).

(b) receiving, in the wireless device and using the connection information for provisioning the ACU program (i.e. the provisioning could be done via a web based provisioning interface, Corrigan: col. 4, line 63 to col. 5, line 10);

(c) provisioning the ACU program based upon the information received in step (b) (Corrigan: col. 4, line 63 to col. 5, line 10);

Corrigan discloses facilitating accesses to VPN services (Corrigan: col. 8, lines 17-30), however it does not explicitly disclose following steps of:

(d) receiving in the wireless device, via the publicly accessible network and using the provisioned ACU program, information for provisioning the VPN program;

(e) provisioning the VPN program based upon the information received in step (d); and

(f) creating a secure communication link using the provisioned VPN program.

Tuomenoksa is relied on for the teaching of (d) receiving in the wireless device, via the publicly accessible network and using the provisioned ACU program, information for provisioning the VPN program (i.e. registering with the network operations center to participate in a VPN, Tuomenoksa: col. 12, lines 42-47);

(e) provisioning the VPN program based upon the information received in step (d) (Tuomenoksa: col. 16, lines 17-38); and

(f) creating a secure communication link using the provisioned VPN program (Tuomenoksa: col. 2, lines 32-36).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of receiving in the wireless device, via the publicly accessible network and using the provisioned ACU program, information for provisioning the VPN program; provisioning the VPN program based upon the information received in step (d); and creating a secure communication link using the provisioned VPN program in the system of Corrigan so as to provide secure VPN for users by enabling authentication and encryption (Tuomenoksa: col. 2, lines 32-36).

b) As to claim 3, the combination of Corrigan and Tuomenoksa discloses determining whether an update to the VPN program is available; receiving the update and implementing the update (i.e. the network operations center provides information and code for configuring processors, such as computers as gateways capable of participating in one or more virtual private networks; administering the configuration of the virtual private networks, distributing changes to the configuration of the virtual private networks; disseminating software updates to the gateways, Tuomenoksa: col. 22, lines 12-30).

c) As to claim 8, the combination of Corrigan and Tuomenoksa discloses determining whether an update is available for at least one additional program; and receiving an update for the at least one additional program (i.e. downloading of software updates and/or information on new services or software versions, Corrigan: col. 7, lines 20-23).

d) As to claim 10, the combination of Corrigan and Tuomenoksa discloses fetching, from one of the one or more remotely-located devices, content or content metadata applicable to the at least one additional program and storing, by the at least one additional program, the fetched content or content metadata (i.e. Email is serviced to mobile users and it can be retrieved from mobile users' mailboxes, Corrigan: col. 4, lines 35-36; col. 6, lines 30-32).

e) As to claim 25, this claim is directed to a hardware implementation of the method of claim 1 and is rejected by a similar rationale applied against claim 1 above.

f) As to claim 27, this claim is directed to a hardware implementation of the method of claim 3 and is rejected by a similar rationale applied against claim 3 above.

g) As to claim 32, this claim is directed to a hardware implementation of the method of claim 8 and is rejected by a similar rationale applied against claim 8 above.

h) As to claim 34, this claim is directed to a hardware implementation of the method of claim 10 and is rejected by a similar rationale applied against claim 10 above.

9. Claims 2 and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Corrigan et al. (6,640,097) in view of Tuomenoksa et al. (7,028,333) and further in view of Forslow (2002/0133534).

a) As to claim 2, the combination of Corrigan and Tuomenoksa discloses the method of claim 1, wherein the information received in step (b) comprises an ACU certificate corresponding to the wireless device (Tuomenoksa: col. 24, lines 14-18). However it is silent on the capability of having the information received in step (d) comprises a VPN certificate corresponding to the wireless device. Forslow is relied on for the teaching of the information received in step (d) comprises a VPN certificate corresponding to the wireless device (Forslow: 0114, Fig. 4A). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of having the information received in step (d) comprises a VPN certificate corresponding to the wireless device in the system of Corrigan and Tuomenoksa, as Forslow teaches, so as to provide a secure network (Forslow: 0015).

b) As to claim 26, this claim is directed to a hardware implementation of the method of claim 2 and is rejected by a similar rationale applied against claim 2 above.

10. Claims 5 and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Corrigan et al. (6,640,097) in view of Tuomenoksa et al. (7,028,333) in view of Balaz et al. (7,100,046).

a) As to claim 5, the combination of Corrigan and Tuomenoksa discloses the method of claim 1, however it is silent on the capability of sending, prior to step (d) a certificate enrollment request for forwarding to an external certification authority (CA). Balaz is relied on for the teaching of sending, prior to step (d), a certificate enrollment request for forwarding to an external certification authority (CA) (i.e. router sends a

GetCertificate request and the certificate is then returned by certificate authority to registration authority, who returns the certificate to router (Balaz: col. 13, lines 15-61). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of sending, prior to step (d), a certificate enrollment request for forwarding to an external certification authority (CA) in the system of Corrigan and Tuomenoksa, as Balaz teaches, so as to provide secure communications by obtaining and maintaining certificates for a VPN (Balaz: col. 1, lines 11-16).

b) As to claim 29, this claim is directed to a hardware implementation of the method of claim 5 and is rejected by a similar rationale applied against claim 5 above.

11. Claims 11 and 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Corrigan et al. (6,640,097) in view of Tuomenoksa et al. (7,028,333) and further in view of Berger et al. (7,114,126).

a) As to claim 11, the combination of Corrigan and Tuomenoksa discloses the method of claim 1, however it is silent on the capability of having the ACU program communicates using a SyncML protocol. Berger is relied on for the teaching of having the ACU program communicates using a SyncML protocol (i.e. architecture 300 includes a file and data synchronization application 310, residing on application server 112, they communicate in SyncML - an XML-based open standard that specifies the protocol for synchronizing heterogeneous devices – in order to exchange and resolve file and data changes between master database and client's data store, see Berger: col. 9, lines 26-35). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of having the ACU program communicates using a SyncML protocol in the system of Corrigan and Tuomenoksa, as Berger teaches, so as to provide a real time observation assessment in computer information gathering and processing.

b) As to claim 35, this claim is directed to a hardware implementation of the method of claim 11 and is rejected by a similar rationale applied against claim 11 above.

12. Claims 12-14 and 36-38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Corrigan et al. (6,640,097) in view of Tuomenoksa et al. (7,028,333) and further in view of Whelan et al. (2004/0203593).

a) As to claim 12, the combination of Corrigan and Tuomenoksa discloses the method of claim 1, however it is silent on the capability of storing, in a configuration record for the VPN program, an Internet Access Point (IAP) to be used when communicating with one of the one or more remotely-located devices on behalf of the VPN program.

Whelan is relied on for the teaching of storing, in a configuration record for the VPN program, an Internet Access Point (IAP) to be used when communicating with one of the one or more remotely-located devices on behalf of the VPN program (i.e. the configuration policy changes dynamically with the access point, whenever a mobile unit connects to a new access point, the system invokes and verifies the proper configuration profile for that access point, see Whelan: 0025).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of storing, in a configuration record for the VPN program, an Internet Access Point (IAP) to be used when communicating with one of the one or more remotely-located devices on behalf of the VPN program in the system of Corrigan and Tuomenoksa, as Whelan teaches, so as to effectively manage hardware and software profiles for mobile units (Whelan: 0011).

b) As to claim 13, Whelan discloses the ACU program communicates using a simple request-response protocol, and wherein a protocol transaction consists of a single request-response pair (i.e. request for updated information (i.e. synchronization), Whelan: 0037, 0065).

c) As to claim 14, Whelan discloses fetching from one of the one or more remotely-located devices, content metadata applicable to the at least one additional program (i.e. the client periodically polls the configuration management server to determine if some of the profile information, software or stored data needs to be synchronized with the information stored on the configuration management server, Whelan: 0078); comparing fetched metadata to locally stored metadata and fetching new or updated content from the one of the one or more remotely-located devices based upon the comparison (i.e. the configuration management client then synchronizes the configuration management profiles, software and data with the profiles, software and data on the configuration management server, Whelan: 0080).

d) As to claim 36, this claim is directed to a hardware implementation of the method of claim 12 and is rejected by a similar rationale applied against claim 12 above.

e) As to claim 37, this claim is directed to a hardware implementation of the method of claim 13 and is rejected by a similar rationale applied against claim 13 above.

f) As to claim 38, this claim is directed to a hardware implementation of the method of claim 14 and is rejected by a similar rationale applied against claim 14 above.

13. Claims 15 and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Corrigan et al. (6,640,097) in view of Tuomenoksa et al. (7,028,333) in view of Whelan et al. (2004/0203593) and further in view of Terada et al. (7,113,983).

a) As to claim 15, the combination of Corrigan, Tuomenoksa and Whelan discloses the method of claim 14, however it is silent on the capability of having the ACU program includes in fetch requests in steps (g) and (i) content identifications (IDs) required by the one of the one or more remotely-located devices. Terada is relied on for the teaching of having the ACU program includes in fetch requests in steps (g) and (i) content identifications (IDs) required by the one of the one or more remotely-located devices (i.e. the client station sends the content ID of the selected program file to the program serving site A, upon receipt of the content ID, site A searches through the content database for content files corresponding to the content ID, ...then sends thus-created information file to the client station, see Terada: col. 12, line 62 to col. 13, line 14). Terada is silent on having the content ID in step (i), content ID is information identifying one particular content, it is necessary in the request message (which is disclosed by Terada), in the response message it could be implemented to confirm the requested item. It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of having the ACU program includes in fetch requests in steps (g) and (i) content identifications (IDs) required by the one of the one or more remotely-located devices in the system of Corrigan, Tuomenoksa and Whelan, as Terada teaches, so as to receive the specified content via a communication network (Terada: col. 2, lines 45-52).

c) As to claim 39, this claim is directed to a hardware implementation of the method of claim 15 and is rejected by a similar rationale applied against claim 15 above.

14. Claims 16 and 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Corrigan et al. (6,640,097) in view of Tuomenoksa et al. (7,028,333) and further in view of Terada et al. (7,113,983)

a) As to claim 16, the combination of Corrigan and Tuomenoksa discloses the method of claim 7, however it is silent on the capability of fetching, from multiple databases in one of the one or more remotely-located devices, metadata about multiple types of content. Terada is relied on for the teaching of fetching, from multiple databases in one of the one or more remotely-located devices, metadata about multiple types of content (i.e. number of program files are prestored in each of sites A-N, and multiples types of content (e.g. music, picture) are sent from these multiple databases, Terada: col. 8, lines 1-20). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of fetching, from multiple databases in one of the one or more remotely-located devices, metadata about multiple types of content in the system of Corrigan and Tuomenoksa, as Terada teaches, so as to download content files over a communication network.

b) As to claim 40, this claim is directed to a hardware implementation of the method of claim 16 and is rejected by a similar rationale applied against claim 16 above.

15. Claims 17 and 41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Corrigan et al. (6,640,097) in view of Tuomenoksa et al. (7,028,333) and further in view of Shannon (6,233,618).

a) As to claim 17, the combination of Corrigan and Tuomenoksa discloses the method of claim 1, however it is silent on the capability of having the ACU program transmits requests containing properties used by one of the one or more remotely-located devices to filter requests. Shannon is relied on for the teaching of having the ACU program transmits requests containing properties used by one of the one or more remotely-located devices to filter requests (i.e. when user's request includes an Internet access address that appears in one of the category/restricted database 208, then user will be denied access to that data, file, applet, web page and so forth, Shannon: col. 8, lines 6-12). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of having the ACU application transmits requests containing properties used by one of the one or more remotely-located devices to filter requests in the system of Corrigan and Tuomenoksa, as Shannon teaches, so as to provide access control based upon the requests (Shannon: col. 4, lines 26-30).

b) As to claim 41, this claim is directed to a hardware implementation of the method of claim 17 and is rejected by a similar rationale applied against claim 17 above.

16. Claims 18 and 42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Corrigan et al. (6,640,097) in view of Tuomenoksa et al. (7,028,333) and further in view of Peterka et al. (2003/0140257).

a) As to claim 18, the combination of Corrigan and Tuomenoksa discloses the method of claim 1, however it is silent on the capability of having messages generated by the ACU program and communicated to one of the one or more remotely-located devices include a message identifier, a target database identifier, and a security level. Peterka is relied on for the teaching of having messages generated by the ACU application and communicated to one of the one or more remotely-located devices include a message identifier, a target database identifier, and a security level (i.e. content provider generates a session rights object (SRO) encapsulates the purchased options (i.e. content ID is included) selected by the consumer, an optional set of content access rules (e.g. security level), the content provider then redirects the viewer to the appropriate caching server (i.e. a target database identifier), Peterka: 0063-0065). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of having messages generated by the ACU application and communicated to one of the one or more remotely-located devices include a message identifier, a target database identifier, and a security level in the system of Corrigan and

Tuomenoksa, as Peterka teaches, so as to securely deliver content to legitimate customers (Peterka: 0013).

b) As to claim 42, this claim is directed to a hardware implementation of the method of claim 18 and is rejected by a similar rationale applied against claim 18 above.

17. Claims 19 and 43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Corrigan et al. (6,640,097) in view of Tuomenoksa et al. (7,028,333) in view of Peterka et al. (2003/0140257) and further in view of Redlich et al. (7,103,915).

a) As to claim 19, the combination of Corrigan, Tuomenoksa and Peterka discloses the method of claim 18, however it is silent on the capability of having a first security level is required to receive configuration information for the VPN program and a second security level is required to receive another type of information. Redlick is relied on for the teaching of having a first security level is required to receive configuration information for the VPN program and a second security level is required to receive another type of information (i.e. the multiple levels and standards or security is introduced, wherein the level of security is determined by the extent of the security sensitive items, selection process, the extent of dispersal to various distributed storage locations; the rules for controlled-release from storage; and the access rules governing the reconstitution of extracts into the secured document, Redlich: col. 8, lines 21-26, users with low level security only are permitted to have access to low level extracted data and users with high level security are permitted to access the entire document, see Redlich: col. 7, lines 12-17). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of having a first security level is required to receive configuration information for the VPN program and a second security level is required to receive another type of information in the system of Corrigan, Tuomenoksa and Peterka, as Redlich teaches, so as to provide flexibility in controlling content delivering (Redlich: col. 8, lines 43-48).

b) As to claim 43, this claim is directed to a hardware implementation of the method of claim 19 and is rejected by a similar rationale applied against claim 19 above.

18. Claims 20 and 44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Corrigan et al. (6,640,097) in view of Tuomenoksa et al. (7,028,333) in view of Peterka et al. (2003/0140257) and further in view of Traversat et al. (2002/0152299).

a) As to claim 20, the combination of Corrigan, Tuomenoksa and Peterka discloses the method of claim 18, however it is silent on the capability of having at least one message generated by the ACU program includes an element indicating that the at least one message is a last message relating to a specific task. Traversat is relied on for the teaching of having at least one message generated by the ACU program includes an element indicating that the at least one message is a last message relating to a specific task (i.e. a message may include an indication that it is the last message, Traversat: 0184). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of having at least one message generated by the ACU program includes an element indicating that the at least one message is a last message relating to a specific task in the system of Corrigan, Tuomenoksa and Peterka, as Traversat teaches, so as to provide reliable connections between peers in a peer-to-peer networking environment, Traversat: 0007).

b) As to claim 44, this claim is directed to a hardware implementation of the method of claim 20 and is rejected by a similar rationale applied against claim 20 above.

19. Claims 21 and 45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Corrigan et al. (6,640,097) in view of Tuomenoksa et al. (7,028,333) in view of Peterka et al. (2003/0140257) and further in view of Whelan et al. (2004/0203593).

a) As to claim 21, the combination of Corrigan, Tuomenoksa and Peterka discloses the method of claim 18, however it is silent on the capability of having the ACU program requests configuration information in a single message. Whelan is relied on for the teaching of having the ACU program requests configuration information in a single message (Whelan: 0093). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of having the ACU program requests configuration information in a single message in the system of Corrigan, Tuomenoksa and Peterka, as Whelan teaches, so as to effectively manage hardware and software profiles for mobile units (Whelan: 0011).

b) As to claim 45, this claim is directed to a hardware implementation of the method of claim 21 and is rejected by a similar rationale applied against claim 21 above.

20. Claims 22, 46, 49 and 51 are rejected under 35 U.S.C. 103(a) as being unpatentable over Corrigan et al. (6,640,097) in view of Tuomenoksa et al. (7,028,333) and further in view of Farnham et al. (2003/0210789).

a) As to claim 22, the combination of Corrigan and Tuomenoksa discloses the method of claim 1, however it is silent on the capability of validating and storing a returned certificate corresponding to one of the one or more remotely-located devices so as to create a trust relationship with that remotely-located device. Farnham is relied on for the teaching of validating and storing a returned certificate corresponding to one of the one or more remotely-located devices so as to create a trust relationship with that remotely-located device (Farnham: 0031, 0080, 0102). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of validating and storing a returned certificate corresponding to one of the one or more remotely-located devices so as to create a trust relationship with that remotely-located device in the system of Corrigan and Tuomenoksa, as Farnham teaches, so as to provide a secure communication link between server and mobile user (Farnham; 0017).

b) As to claim 49, the combination of Corrigan, Tuomenoksa and Farnham discloses the method of claim 22, wherein step (g) includes requiring input of multiple characters from a user of the wireless device (i.e. mobile users inputs access security codes when requesting service (Corrigan: col. 4, lines 2-3).

c) As to claim 46, this claim is directed to a hardware implementation of the method of claim 22 and is rejected by a similar rationale applied against claim 22 above.

d) As to claim 51, this claim is directed to a hardware implementation of the method of claim 49 and is rejected by a similar rationale applied against claim 49 above.

21. Claims 23-24, 47, 50 and 52 are rejected under 35 U.S.C. 103(a) as being unpatentable over Corrigan et al. (6,640,097) in view of Tuomenoksa et al. (7,028,333) in view of Farnham et al. (2003/0210789) and further in view of Srinivasan (2003/0126085).

a) As to claim 23, the combination of Corrigan, Tuomenoksa and Farnham discloses the method of claim 22, however it is silent on the capability of using the certificate stored in step (g) to validate subsequent responses from that remotely-located device. Srinivasan is relied on for the teaching of using the stored certificate to validate subsequent responses from that remotely-located device (i.e. the information cached remains in the recipient's local keystore and is available for processing of subsequently received message, Srinivasan: 0047). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of using the stored certificate to validate subsequent responses from that remotely-located device in the system of Corrigan, Tuomenoksa and Farnham, as Srinivasan teaches, so as to make message communication more efficient without repeating authentication of certificates, Srinivasan: 0047).

b) As to claim 24, the combination of Corrigan, Tuomenoksa and Farnham and Srinivasan discloses the method of claim 23, wherein the certificate corresponding to the one of the one or more remotely-located devices is validated based on a hash calculated over an entire ACU message, except for a signature element of that ACU message (e.g. a cryptographic digest of the message (i.e. excluding signature element), Srinivasan: 0003, 0040), the hash is signed with a private key held by the one of the one or more remotely-located devices (i.e. sender A encrypts (i.e. signs) a cryptographic digest of the message using its private key, Srinivasan: 0003), and the certificate corresponding to the one of the one or more remotely-located devices is included in a first response from the one of the one or more remotely-located devices and is used by wireless device to verify the signature and identify and authenticate a sender (i.e. assuming that a recipient B of the message has the sender's public key, the recipient can apply the sender's public key to decrypt the message digest, then by comparing the decrypted digest to a computed digest of the received message, the recipient can authenticate the message to verify that the message originated with sender A and that the message was not altered after sender A sent it, Srinivasan: 0003).

c) As to claim 50, the combination of Corrigan, Tuomenoksa and Farnham discloses the method of claim 22, however it is silent on the capability of having the multiple characters are a portion of an identifier for the certificate corresponding to one of the one or more remotely-located device. Srinivasan is relied on for the teaching of having the multiple characters are a portion of an identifier for the certificate corresponding to one of the one or more remotely-located device (Srinivasan: 0010, Fig. 3A). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of having the multiple characters are a portion of an identifier for the certificate corresponding to one of the one or more remotely-located device in the system of Corrigan, Tuomenoksa and Farnham, as Srinivasan teaches, so as to dynamically authenticate certificate, Srinivasan: 0011).

d) As to claim 47, this claim is directed to a hardware implementation of the method of claim 23 and is rejected by a similar rationale applied against claim 23 above.

e) As to claim 52, this claim is directed to a hardware implementation of the method of claim 50 and is rejected by a similar rationale applied against claim 50 above.

## *Conclusion*

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dieu Nguyen whose telephone number is 571-272-3873.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MinhDieu Nguyen
Patent Examiner
2/15/08